

U.S. Application Serial No. 09/447,500

REMARKS

The Applicant and the undersigned thank Examiner Vaughan for the careful review of this application. Claims 1-40 have been rejected and Claim 40 has been objected by the Examiner. Upon entry of this amendment, Claims 1-40 remain pending in this application. The independent claims are Claims 1, 18, 26, 31, and 32. Consideration of the present application is respectfully requested in light of the above amendments to the application and in view of the following remarks.

Objection to the Drawings

The drawings stand objected to by the Examiner because in Figures 1-9, the lines, numbers, and letters are not uniformly thick and well defined. The Official Draftsperson also notes that the figure legends are unclear.

Attached hereto are proposed drawing corrections and a letter to the official draftsperson pursuant to M.P.E.P. § 608.02(r) addressing these corrections made by the Applicant. The Examiner is requested to approve these proposed drawing corrections.

Applicant attaches herewith eight (8) sheets of proposed drawing corrections with changes highlighted with dashed circles and solid circles as permitted by M.P.E.P. § 608.02(v) ("with changes otherwise highlighted"). The Applicant proposes to remove all borders and grid lines that were present in the originally filed drawings. The Applicant wants the record for this application to be clear that the Applicant created the drawings informally on engineering paper. Specifically, the Applicant created the drawings on "AMPAD" brand paper. Therefore, the Applicant wants confirmation from the Examiner and the Official Draftsperson that such removal of lines and the brand name of "AMPAD" will be acceptable and will not raise any issues.

The attached proposed drawing corrections have been highlighted with dashed circles to indicate what elements of the attached drawings will be removed. On several of the drawings, the brand of "AMPAD" will be removed as highlighted with the dashed circles. Also, drawing sheet numbers that are enclosed with solid circles are proposed to be added to each drawing sheet. The Applicant notes that these sheet numbers will not be placed in solid circles for the corrected drawings when they are filed at a later date. Consideration and approval of the

U.S. Application Serial No. 09/447,500

attached proposed drawing corrections are respectfully requested. Upon approval of the attached proposed drawing corrections, the Applicant can employ the services of an Official draftsperson if required by the Examiner.

Objection to the Claims

Claim 40 stands objected to by the Examiner as the Examiner discovered a misspelled word. Specifically, in claim 40, it was recommended by the Examiner to change the word, "pervious," to --previous--.

The Applicant appreciates the Examiner's helpful suggestion and has amended Claim 40 in light of this suggestion. Reconsideration and withdrawal of this drawing objection are respectfully requested.

Claim Rejections under 35 U.S.C. § 112

The Examiner has rejected Claim 15 under 35 U.S.C. § 112, second paragraph. Specifically, the Examiner states that the phrase, "e.g. (for example)" renders Claim 15 indefinite because its unclear whether the limitations following the phrase are part of the claimed invention.

The Applicant has amended independent Claim 15 in accordance with the Examiner's helpful comments. Reconsideration and withdrawal of this rejection are respectfully requested.

Claim Rejections under 35 U.S.C. § 102(b) and § 103(a)

The Examiner rejected Claims 1-3, 18-22, 24-28, 31, 32, 35, 36, 39, and 40 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,345,595 to Johnson et al (hereinafter the "Johnson reference"). The Examiner rejected Claims 4-7, 10-14, 16-17, 23, 29-30, 33-34 and 37 under 35 U.S.C. § 103(a) as being unpatentable over the Johnson reference in view of U.S. Patent No. 5,414,833 to Hershey et al (hereinafter the "Hershey reference").

The Examiner rejected Claim 8 under 35 U.S.C. § 103(a) as being unpatentable over the Johnson reference in view of U.S. Patent No. 5,475,839 to Watson et al (hereinafter the "Watson reference"). The Examiner rejected Claim 8 under 35 U.S.C. § 103(a) as being

U.S. Application Serial No. 09/447,500

unpatentable over the Johnson reference in view of the Watson reference, and further in view of a printed publication entitled, "Using the CamNet BBS" (hereinafter, the "CamNet reference").

The Examiner rejected Claim 15 under 35 U.S.C. § 103(a) as being unpatentable over the Johnson reference in view of the Hershey reference, and further in view of a printed publication entitled, "NASA Automated Systems Incident Response Capability (NASIRC)" (hereinafter, the "NASIRC reference"). The Examiner rejected Claim 38 under 35 U.S.C. § 103(a) as being unpatentable over the Johnson reference in view of a printed publication entitled, "Packages in the net directory" (hereinafter the "Packages reference"). The Applicant respectfully offers remarks to traverse these pending rejections.

Independent Claim 1

The rejection of Claim 1 is respectfully traversed. It is respectfully submitted that the Johnson and Hershey references fail to describe, teach, or suggest (1) analyzing computer data transmissions to determine what type of data is contained in the computer data transmissions; (2) modifying an alert variable based on the computer data transmissions originating from one or more suspect computer nodes; (3) triggering a first response when said alert variable reaches a first predetermined threshold level; and (4) triggering a second response when the alert variable reaches a second predetermined threshold level, as recited in amended independent Claim 1.

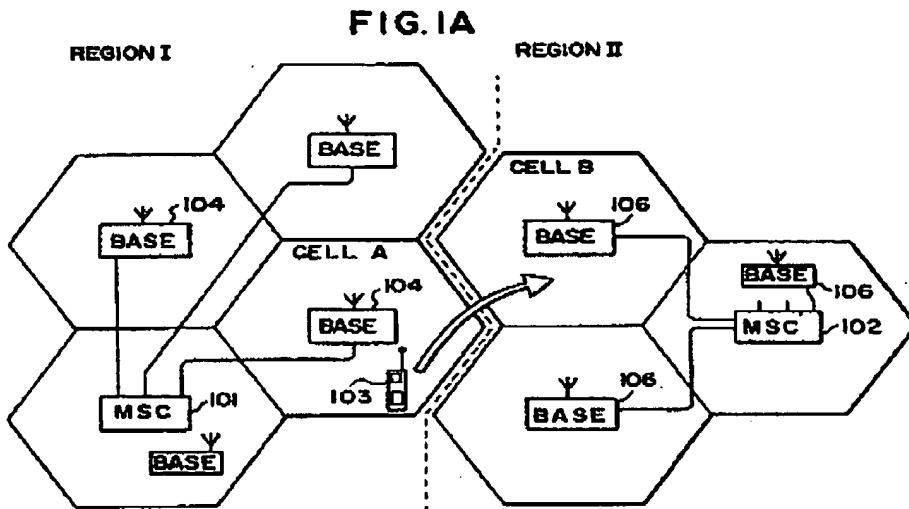
The Applicants respectfully submit that the Johnson patent is not analogous art according to M.P.E.P. § 2141.01(a) (8th Ed., Rev. 1, February 2003) which states the following:

"TO RELY ON A REFERENCE UNDER 35 U.S.C. 103, IT
MUST BE ANALOGOUS PRIOR ART.

The Examiner must determine what is 'analogous prior art' for the purpose of analyzing the obviousness of the subject matter at issue. In order to rely on a reference as a basis for rejection of an Applicant's invention, the reference must either be in the field of Applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the inventor was concerned. In re Oetiker, 977 F2d 1443, 24 USPQ 2d 1443, 1445 (Fed. Cir. 1992)."

U.S. Application Serial No. 09/447,500

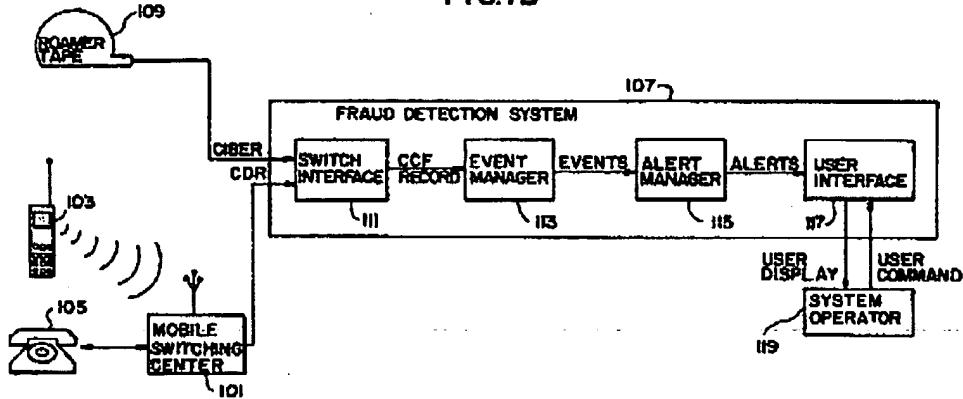
The Johnson patent describes technology for monitoring telecommunication systems and more specifically, system for detecting potentially fraudulent telecommunication system usage. See Johnson reference, column 1, lines 8-11. In Figure 1A of the Johnson reference (reproduced below), a diagram illustrating a typical cellular telecommunications network is presented.



A first fixed geographic REGION I made of several cells is served by a first mobile switching center (MSC) 101 that is coupled to several base stations 104. Each base station 104 provides coverage for a particular cell within a geographic region. See Johnson reference, column 5, lines 9-15. Referring to Figure 1B of Johnson (reproduced below), this figure illustrates a fraud detection system 107 that includes a switch interface 111 that translates a call detail record (CDR) into a CCF format understandable to the fraud detection system 107. CDR records for both cellular originated and cellular terminated calls are fed into the switch interface 111 both from the mobile switching centers (MSCs) 101 directly and from a roamer tape 109.

U.S. Application Serial No. 09/447,500

FIG.1B



Each CCF record is passed to an event manager 113 that performs a number of checks to compare the present CCF record both with past subscriber specific usage information and with certain predetermined conditions to determine whether this particular CCF record should trigger the event manager 113 to generate an "event."

One of ordinary skill in the art recognizes that the telecommunications system of the Johnson reference is not in the computer security field of Applicant's endeavor and is not reasonably pertinent to the particular problem of computer network security with which the inventor of the present application was concerned. Simply stated, the Johnson reference does not provide any teaching of analyzing computer data transmissions to determine what type of data is contained in the computer data transmissions as recited in amended independent Claim 1.

Instead, the Johnson reference teaches analyzing call detail records (CDRs) which are not related to computer data transmissions. The Johnson reference can be properly characterized as a security system for a circuit switched network while the Applicants technology can be properly characterized as a security system for a packet switched network. One of ordinary skill in the art would not refer to a security system of a circuit switched network to address problems or issues with a packet switched network. Therefore, the Johnson reference is not analogous art and cannot be relied on as a basis for rejection of the Applicant's invention.

To make up for several deficiencies of the Johnson reference, the Examiner relies upon the Hershey reference. Specifically, the Examiner admits that the Johnson reference does

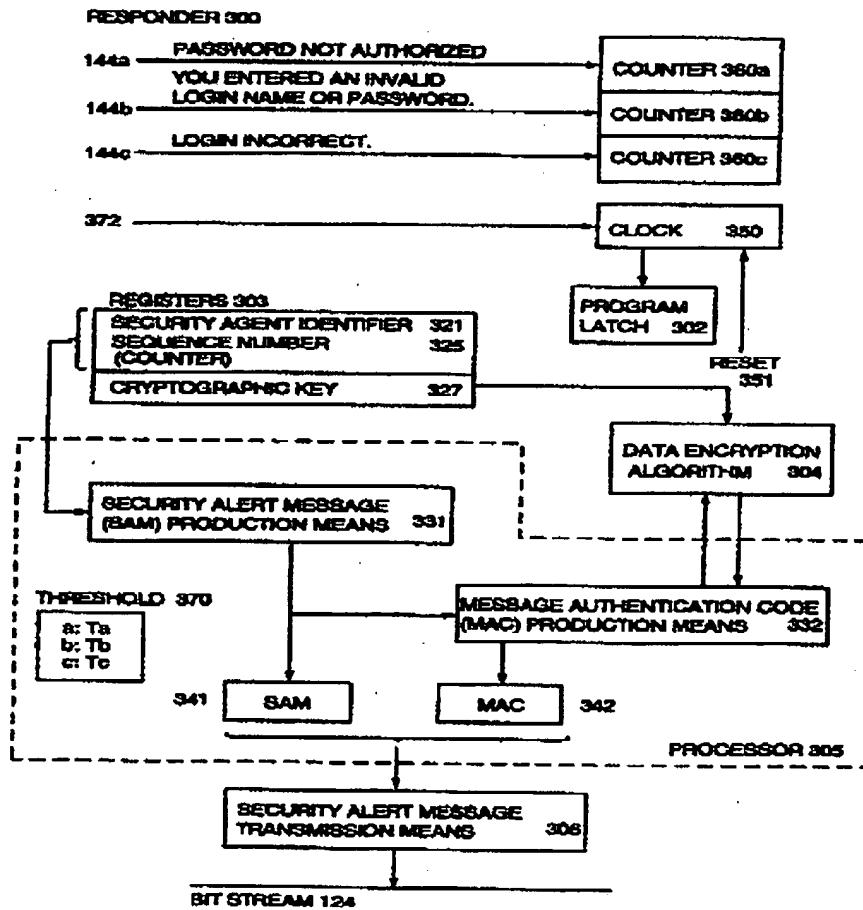
U.S. Application Serial No. 09/447,500

not provide any teachings of recording data transmissions in a log file and actively scanning suspect nodes. The Examiner relies on the Hershey reference to provide these teachings.

The Hershey reference describes pattern matching finite state machines that do not determine the type of data contained in a data transmission. Specifically, the Hershey reference in Figure 10 (reproduced below) describes an intrusion detector and responder 300 that has pattern alarms 144a, 144b, 144c that review data transmissions for three characteristic patterns, specified in double quotation marks listed below:

1. "Password Not Authorized" - 144a
2. "You entered an invalid login name or password." - 144b
3. "Login incorrect." - 144c

FIG. 10



U.S. Application Serial No. 09/447,500

Counters 360 track how many times each of the characteristic patterns are detected by respective pattern alarms 144. At some point, each of the counters 360 are reset. See Hershey reference, column 21, lines 55-68. This intrusion detector and responder 300 of the Hershey reference is different than analyzing computer data transmissions to determine what type of data is contained in the computer data transmissions, as recited in the amended independent Claim 1.

Specifically, the present application states on page 32, lines 1-6, that the analysis module 250 as illustrated in Figure 2B (reproduced below) determines the type of data contained in a packet. For example, the analysis module can determine whether the packet is a ping, login request, etc.

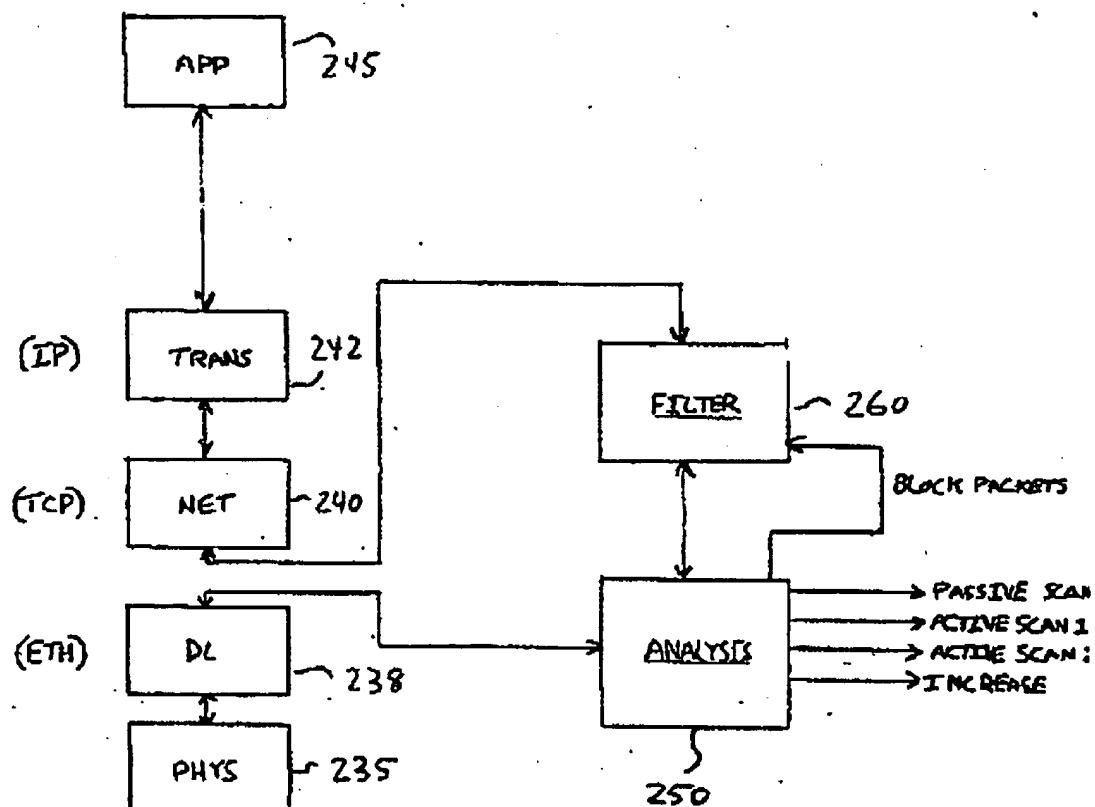


FIG 2B

Such a determination of what type of data is contained in the computer data transmissions as recited in independent Claim 1 is opposite to the pattern matching state machine system of the

U.S. Application Serial No. 09/447,500

Hershey reference that includes pattern alarms 144a, 144b, 144c that review data transmissions for characteristic patterns. A simple example that demonstrates the differences between the invention as recited in amended independent Claim 1 and the system described by the Hershey reference is as follows: a computer data transmission containing "Password Not Authorized" would trigger a response by the Hershey reference, meanwhile, a response would not be generated by the invention as described in amended independent Claim 1.

In light of the differences between the claims and the references mentioned above, one of ordinary skill in the art recognizes that the Johnson and Hershey references, alone or in combination, cannot anticipate or render obvious the recitations as set forth in amended independent Claim 1. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Independent Claim 18

The rejection of Claim 18 is respectfully traversed. It is respectfully submitted that the Johnson and Hershey references fail to describe, teach, or suggest (1) analyzing computer data transmissions to determine what type of data is contained in the computer data transmissions; (2) modifying a first suspect-specific alert variable based on the computer data transmissions originating from a first suspect computer node; (3) modifying a second suspect-specific alert variable based on the computer data transmissions originating from a second suspect computer node; and (4) triggering a suspect-specific response when either of the suspect-specific alert variables reach a predetermined threshold level, as recited in amended independent Claim 18.

As noted above in the section addressing independent Claim 1, the Johnson reference teaches analyzing call detail records (CDRs) which are not related to computer data transmissions. The Johnson reference can be properly characterized as a security system for a circuit switched network while the Applicants technology can be properly characterized as a security system for a packet switched network. One of ordinary skill in the art would not refer to a security system of a circuit switched network to address problems or issues with a packet switched network. Therefore, the Johnson reference is not analogous art and cannot be relied on as a basis for rejection of the Applicant's invention.

U.S. Application Serial No. 09/447,500

Regarding the Hershey reference, as noted above, a determination of what type of data is contained in the computer data transmissions as recited in independent Claim 1 is opposite to the pattern matching state machine system of the Hershey reference that includes pattern alarms 144a, 144b, 144c that review data transmissions for characteristic patterns. A simple example that demonstrates the differences between the invention as recited in amended independent Claim 1 and the system described by the Hershey reference is as follows: a computer data transmission containing "Password Not Authorized" would trigger a response by the Hershey reference, meanwhile, a response would not be generated by the invention as described in amended independent Claim 18.

In light of the differences between the claims and the references mentioned above, one of ordinary skill in the art recognizes that the Johnson and Hershey references, alone or in combination, cannot anticipate or render obvious the recitations as set forth in amended independent Claim 18. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Independent Claim 26

The rejection of Claim 26 is respectfully traversed. It is respectfully submitted that the Johnson and Hershey references fail to describe, teach, or suggest (1) storing a plurality of suspect-specific alert variables for a plurality of computer network nodes; (2) modifying a network alert variable based on the value of each of said plurality of suspect-specific alert variables; and (3) triggering a network response when said network alert variable reaches a predetermined threshold level, as recited in amended independent Claim 26.

As noted above in the section addressing independent Claim 1, the Johnson reference teaches analyzing call detail records (CDRs) which are not related to computer data transmissions. The Johnson reference can be properly characterized as a security system for a circuit switched network while the Applicants technology can be properly characterized as a security system for a packet switched network. One of ordinary skill in the art would not refer to a security system of a circuit switched network to address problems or issues with a packet switched network. Therefore, the Johnson reference is not analogous art and cannot be relied on as a basis for rejection of the Applicant's invention.

U.S. Application Serial No. 09/447,500

Regarding the Hershey reference, this reference describes a pattern matching state machine system that includes pattern alarms 144a, 144b, 144c that review data transmissions for characteristic patterns. The Hershey reference does not provide any teaching of modifying a network alert variable based on the value of each of said plurality of suspect-specific alert variables and triggering a network response when said network alert variable reaches a predetermined threshold level, as recited in amended independent Claim 26.

In light of the differences between the claims and the references mentioned above, one of ordinary skill in the art recognizes that the Johnson and Hershey references, alone or in combination, cannot anticipate or render obvious the recitations as set forth in amended independent Claim 26. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Independent Claim 31

The rejection of Claim 31 is respectfully traversed. It is respectfully submitted that the Johnson and Hershey references fail to describe, teach, or suggest (1) storing a plurality of overall alert variables for a plurality of computer network nodes; (2) modifying a network alert variable based on the value of each of said plurality of overall alert variables; and (3) triggering a network response when the network alert variable reaches a predetermined threshold level, as recited in amended independent Claim 31.

As noted above in the section addressing independent Claim 1, the Johnson reference teaches analyzing call detail records (CDRs) which are not related to computer data transmissions. The Johnson reference can be properly characterized as a security system for a circuit switched network while the Applicants technology can be properly characterized as a security system for a packet switched network. One of ordinary skill in the art would not refer to a security system of a circuit switched network to address problems or issues with a packet switched network. Therefore, the Johnson reference is not analogous art and cannot be relied on as a basis for rejection of the Applicant's invention.

Regarding the Hershey reference, this reference describes a pattern matching state machine system that includes pattern alarms 144a, 144b, 144c that review data transmissions for characteristic patterns. The Hershey reference does not provide any teaching of the combination

U.S. Application Serial No. 09/447,500

of (1) storing a plurality of overall alert variables for a plurality of computer network nodes; (2) modifying a network alert variable based on the value of each of said plurality of overall alert variables; and (3) triggering a network response when the network alert variable reaches a predetermined threshold level, as recited in amended independent Claim 31.

In light of the differences between the claims and the references mentioned above, one of ordinary skill in the art recognizes that the Johnson and Hershey references, alone or in combination, cannot anticipate or render obvious the recitations as set forth in amended independent Claim 31. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Independent Claim 32

The rejection of Claim 32 is respectfully traversed. It is respectfully submitted that the Johnson and Hershey references fail to describe, teach, or suggest (1) analyzing a first event from a suspect computer node to determine what type of data is contained in the event; (2) recording the first event in a first data structure having an event count value; (3) analyzing a second event from the computer suspect node to determine what type of data is contained in the event, the second event being of a same type as the first event; and (4) recording the second event in the first data structure and incrementing the count value if the second event occurs within a predetermined window of time after the first event, as recited in amended independent Claim 32.

As noted above in the section addressing independent Claim 1, the Johnson reference teaches analyzing call detail records (CDRs) which are not related to computer data transmissions. The Johnson reference can be properly characterized as a security system for a circuit switched network while the Applicants technology can be properly characterized as a security system for a packet switched network. One of ordinary skill in the art would not refer to a security system of a circuit switched network to address problems or issues with a packet switched network. Therefore, the Johnson reference is not analogous art and cannot be relied on as a basis for rejection of the Applicant's invention.

Regarding the Hershey reference, as noted above, a determination of what type of data is contained in the computer data transmissions as recited in independent Claim 32 is opposite to the pattern matching state machine system of the Hershey reference that includes

U.S. Application Serial No. 09/447,500

pattern alarms 144a, 144b, 144c that review data transmissions for characteristic patterns. A simple example that demonstrates the differences between the invention as recited in amended independent Claim 1 and the system described by the Hershey reference is as follows: a computer data transmission containing "Password Not Authorized" would trigger a response by the Hershey reference, meanwhile, a response would not be generated by the invention as described in amended independent Claim 32.

In light of the differences between the claims and the references mentioned above, one of ordinary skill in the art recognizes that the Johnson and Hershey references, alone or in combination, cannot anticipate or render obvious the recitations as set forth in amended independent Claim 32. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Dependent Claims 2-17, 19-25, 27-30, and 33-40

The Applicant respectfully submits that Claims 2-17, 19-25, 27-30, and 33-40 are allowable because the independent claims from which they depend are patentable over the cited references. The Applicant also respectfully submits that the recitations of these dependent claims are of patentable significance.

Regarding Claim 8, to make up for the increased authentication deficiency of the Johnson reference, the Examiner relies on the Watson reference to provide such a teaching. Because the Johnson reference is no longer applicable to the amended claims, the Examiner's argument with respect to the Watson reference has been rendered moot. However, the Applicant points out that the Watson reference fails to provide any teaching of the combination of (1) analyzing computer data transmissions to determine what type of data is contained in the computer data transmissions; (2) modifying an alert variable based on the computer data transmissions originating from one or more suspect computer nodes; (3) triggering a first response when said alert variable reaches a first predetermined threshold level; and (4) triggering a second response when the alert variable reaches a second predetermined threshold level, as recited in amended independent Claim 1.

Regarding Claim 9, to make up for the two or more logins deficiency of the Johnson reference, the Examiner relies on the CamNet reference to provide such a teaching.

U.S. Application Serial No. 09/447,500

Because the Johnson reference is no longer applicable to the amended claims, the Examiner's argument with respect to the CamNet reference has been rendered moot. However, the Applicant points out that the Watson reference fails to provide any teaching of the combination of (1) analyzing computer data transmissions to determine what type of data is contained in the computer data transmissions; (2) modifying an alert variable based on the computer data transmissions originating from one or more suspect computer nodes; (3) triggering a first response when said alert variable reaches a first predetermined threshold level; and (4) triggering a second response when the alert variable reaches a second predetermined threshold level, as recited in amended independent Claim 1.

Regarding Claim 15, to make up for the deficiency of Johnson for having a transmission which retrieves information about the computer network node, the Examiner relies upon the NASIRC reference to provide such a teaching. Because the Johnson reference is no longer applicable to the amended claims, the Examiner's argument with respect to the CamNet reference has been rendered moot. However, the Applicant points out that the CamNet reference fails to provide any teaching of the combination of (1) analyzing computer data transmissions to determine what type of data is contained in the computer data transmissions; (2) modifying an alert variable based on the computer data transmissions originating from one or more suspect computer nodes; (3) triggering a first response when said alert variable reaches a first predetermined threshold level; and (4) triggering a second response when the alert variable reaches a second predetermined threshold level, as recited in amended independent Claim 1.

Regarding Claim 38, to make up for ping event type of the Johnson reference, the Examiner relies upon the Packages reference. Because the Johnson reference is no longer applicable to the amended claims, the Examiner's argument with respect to the Packages reference has been rendered moot. However, the Applicant points out that the Packages reference fails to provide any teaching of the combination of (1) analyzing a first event from a suspect computer node to determine what type of data is contained in the event; (2) recording the first event in a first data structure having an event count value; (3) analyzing a second event from the computer suspect node to determine what type of data is contained in the event, the second event being of a same type as the first event; and (4) recording the second event in the first data

U.S. Application Serial No. 09/447,500

structure and incrementing the count value if the second event occurs within a predetermined window of time after the first event, as recited in amended independent Claim 32.

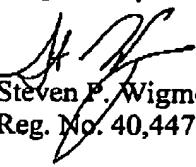
Accordingly, reconsideration and withdrawal of the rejections of these dependent claims are respectfully requested.

Conclusion

The foregoing is submitted as a full and complete response to the Office Action mailed on September 30, 2003. The Applicant and the undersigned thank Examiner Vaughn for consideration of these remarks. The Applicant has amended the claims and has submitted remarks to traverse rejections of Claims 1-40. The Applicant respectfully submits that the present application is in condition for allowance. Such action is hereby courteously solicited.

If the Examiner believes that there are any issues that can be resolved by a telephone conference, or that there are any formalities that can be corrected by an Examiner's amendment, please contact the undersigned in the Atlanta Metropolitan area (404) 572-2884.

Respectfully submitted,


Steven P. Wigmore
Reg. No. 40,447

King & Spalding LLP
45th Floor, 191 Peachtree Street, N.E.
Atlanta, GA 30303
404.572.4600
K&S Docket: 05456.105034